RSAC 2025 Conference

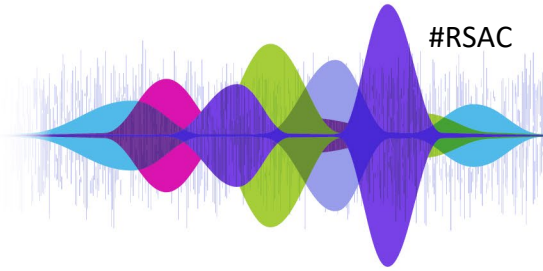
Many Voices.
One Community.

SESSION ID: IDY-M06

Carrier Tokens — A Game-Changer Towards SMS OTP Free World!

Kazi Wali Ullah

Senior Security Technology Specialist | CISSP
Ericsson
https://www.linkedin.com/in/kaziullah/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

© Ericsson 2025. All Rights Reserved. No part of this presentation may be reproduced in any form without the written permission of the copyright owner.
ERICSSON and the Ericsson logotype are the trademarks or registered trademarks of Telefonaktiebolaget LM Ericsson.

Agenda

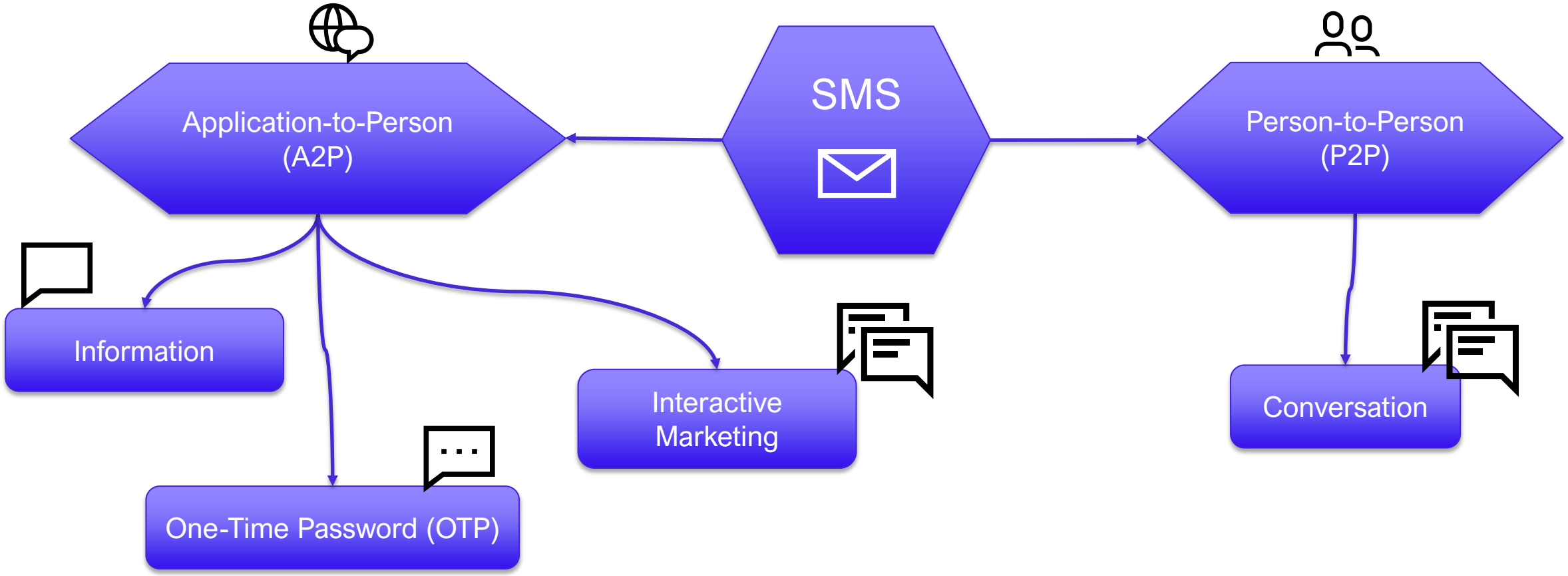
- The famous SMS OTP – a recap
- Current Number Verification mechanism
- Evolution of number verification using Carrier Tokens
- How it works in practice – a visual depiction
- The road ahead…

RSAC 2025 Conference

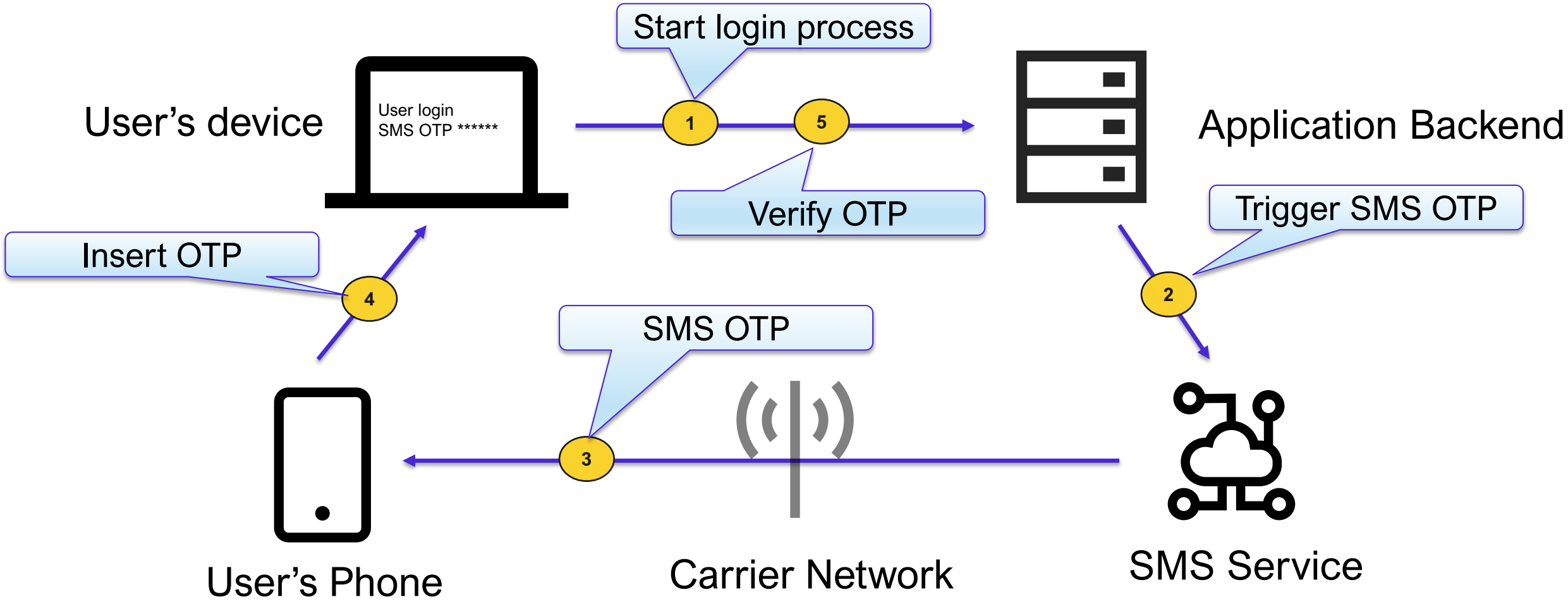
Revisiting SMS

Many Voices.
One Community.

SMS use-cases: an overview



SMS OTP


Start login process
User's device
User login
SMS OTP ******
1
5
Verify OTP
Application Backend
Trigger SMS OTP
Insert OTP
4
2
SMS OTP
3
User's Phone
Carrier Network
SMS Service

SMS OTP – global prevalence

SMS being a built-in global standard and available across all CSPs

Familiarity and comfortable way of communication

Global reach and scale

Affordability

SMS – security pitfalls

- Several attacks demonstrated
  - Social engineering attacks
    - SIM swap attack
    - tricking victims into revealing their OTPs
  - SMS hijacking using SS7 flaw
- Lack of e2e encryption
- Privacy issue
- Fraud – Artificially Inflated Traffic (AIT) / traffic pumping

Root cause - SMS was not designed with security use cases in mind!

SMS OTP – regulatory aspects

NIST 800-63B – SMS OTPs can be considered suitable for the lowest Authenticator Assurance Level (AAL1) but not recommended for higher assurance levels (AAL2 or AAL3)

PSD2* – While PSD2 does not outright prohibit the use of SMS OTPs, but the recommendation is that SMS OTPs meets strong customer authentication

**PSD2 – EU Payment Services Directive*

TECHWIRE ASIA

News Podcasts Popular Insights

ASIA

Malaysia is migrating from the usage of SMS OTP. Is biometrics the answer?

Dashveenjit Kaur September 27, 2022

The Register

Singapore's banks to ditch texted one-time passwords

All these creates a push and pull in the market for a more secure solution

RSAC 2025 Conference

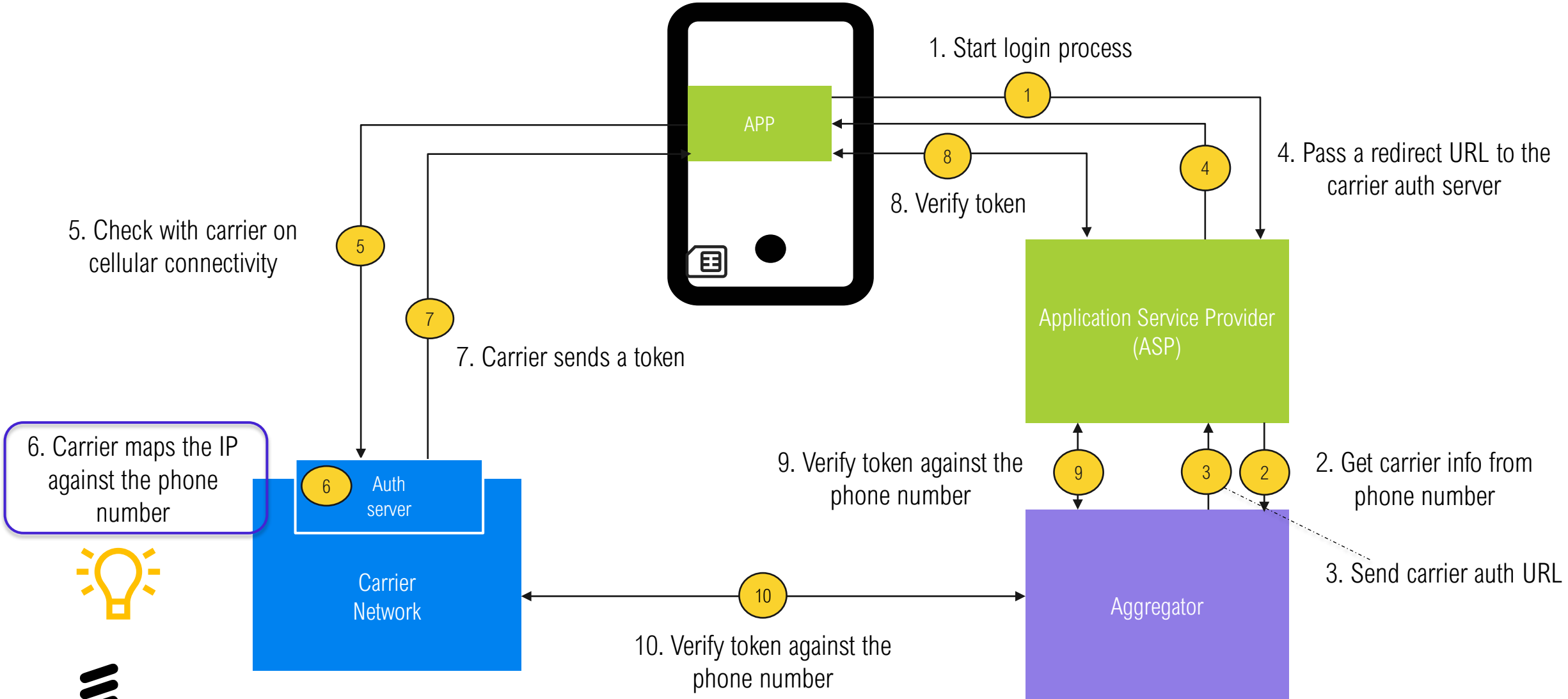
Introducing CAMARA Number Verification API

Many Voices.
One Community.

CAMARA Number Verification API

- CAMARA – The Telco Global API Alliance
- “The ‘Number Verification’ API is a service that enables businesses to seamlessly confirm the ownership of a mobile phone number and retrieve the number directly from the user’s device.”
- Also known as “Silent Authentication” in the industry

How it works?



ERICSSON

RSAC 2025 Conference

Security & privacy improvements over SMS OTP

- Several attacks demonstrated
  - Social engineering attacks
    - SIM swap attack → Possibility to detect SIM swap via another API
    - tricking victims into revealing their OTPs → Nothing to ask for anymore
  - SMS hijacking using SS7 flaw → Not possible as there is no more SMS to deliver
- Lack of e2e encryption → Not applicable as no data is sent via other services like SMS
- Privacy issue → Not applicable as no data to read like in SMSs
- Fraud – Artificially Inflated Traffic (AIT) / traffic pumping → Less incentive, less fraud

SMS was not designed with security use cases in mind, but modern number verification mechanism is!

Key facts – CAMARA Number Verification

Pros	Cons
Enhanced security and privacy	Needs cellular connectivity (e.g. does not work over WiFi)
Significantly Improved UX	SDK dependance

While this mechanism solves the biggest issues of SMS OTP, these limitations leaves room for a better alternative!

RSAC™ 2025 Conference

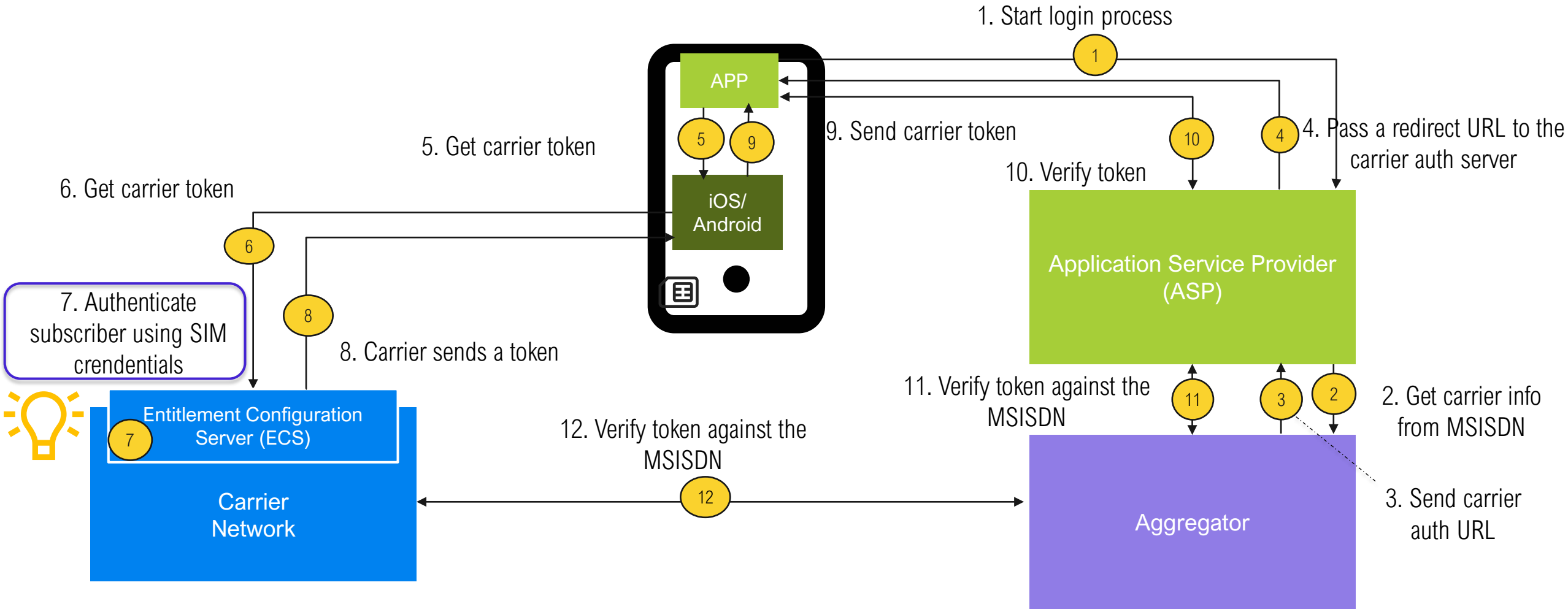
Introducing Carrier Token-based “Enhanced Number Verification”

Many Voices.
One Community.

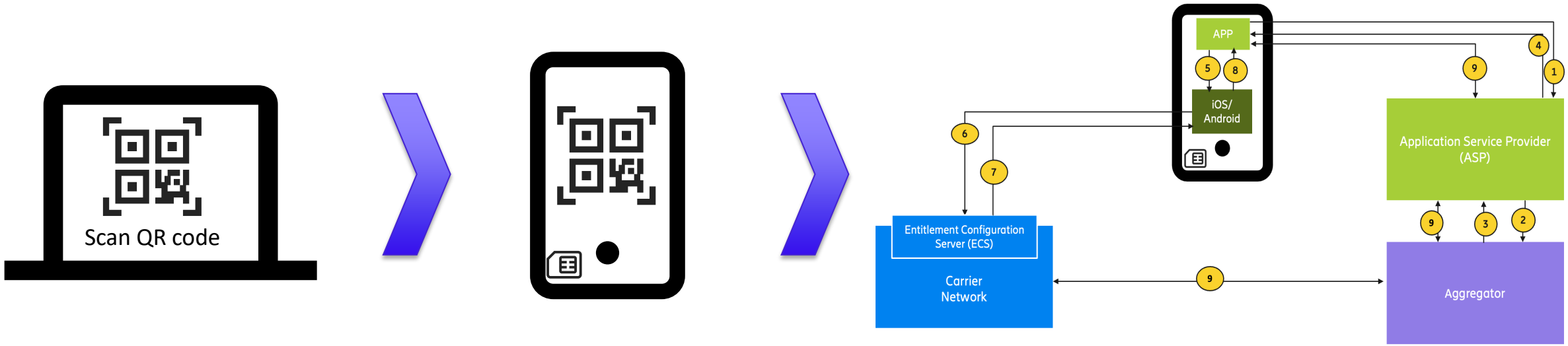
Carrier/Operator Tokens

- A token that is issued by the carrier/operator after subscriber authentication
  - A typical OAuth2-based token
- Both iOS and Android supports this carrier/operator tokens today
  - Both have the clients built into the OS to retrieve a token from the carrier
- Important: tokens operate in a bit different way in iOS and Android ecosystem

Number verification using carrier tokens -native app/browser case



Number verification using carrier tokens - companion device case



Step 1: Start at the consumption device

Step 2: Scan the QR code on your phone

Step 3: Phone does the number verification

Key facts – Enhanced Number Verification

Pros

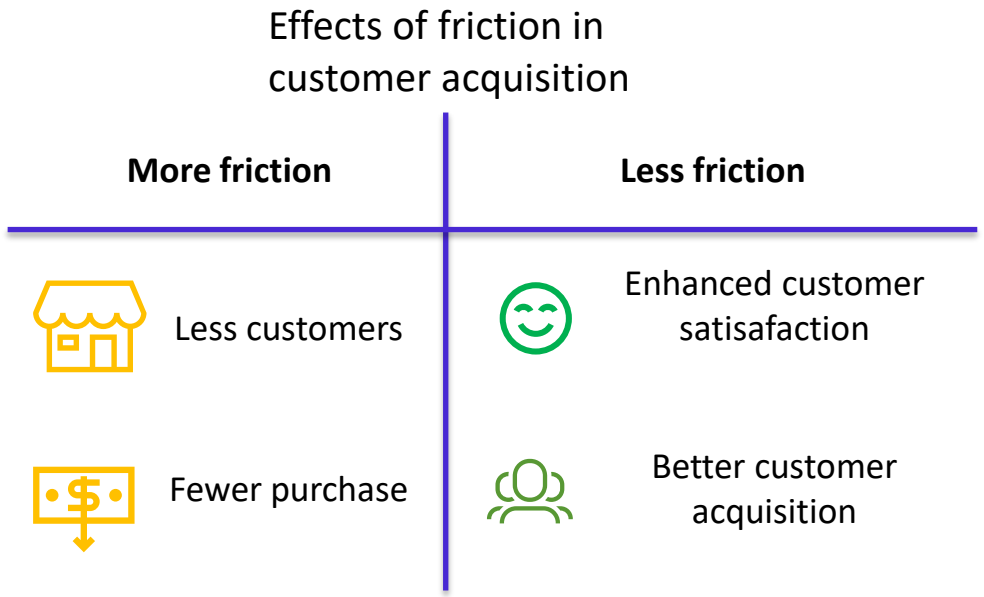
- Enhanced security and privacy
- Significantly Improved UX

Pros

- No need to switch to cellular connectivity (e.g. works over WiFi)
- No need for SDK dependance

UX matters

Friction and the UX



Use case analysis

- UC: a user funnel for the loan request process
  - Request a loan
  - Fill in loan details
  - Confirm loan details
  - Enter the OTP code to finalise the process.
- 22% of drop offs came from the OTP identification in the session funnel they created.*

* *Use Case - OTP Validation - Removing Friction*

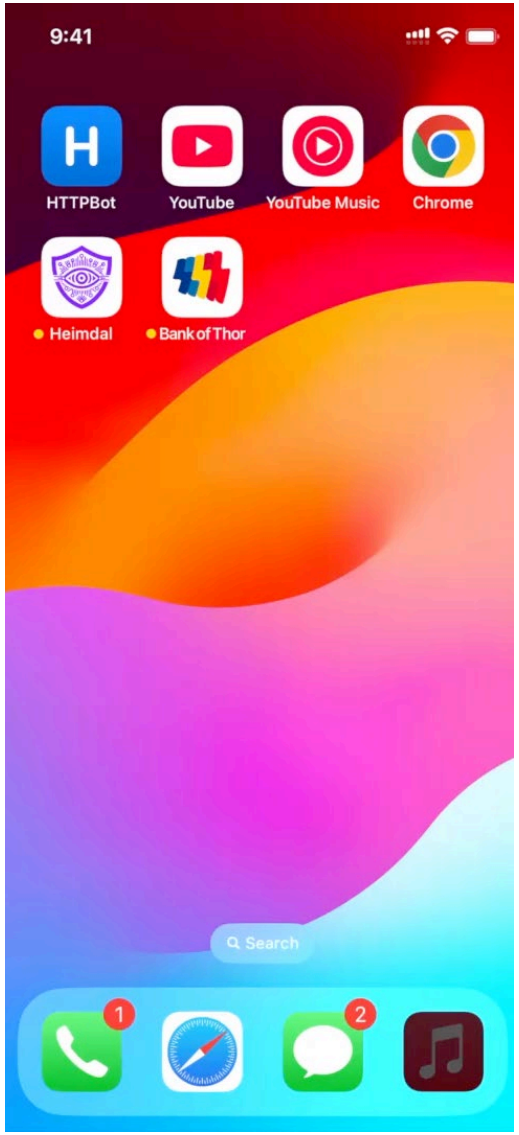
RSAC 2025 Conference

Let’s watch a demo

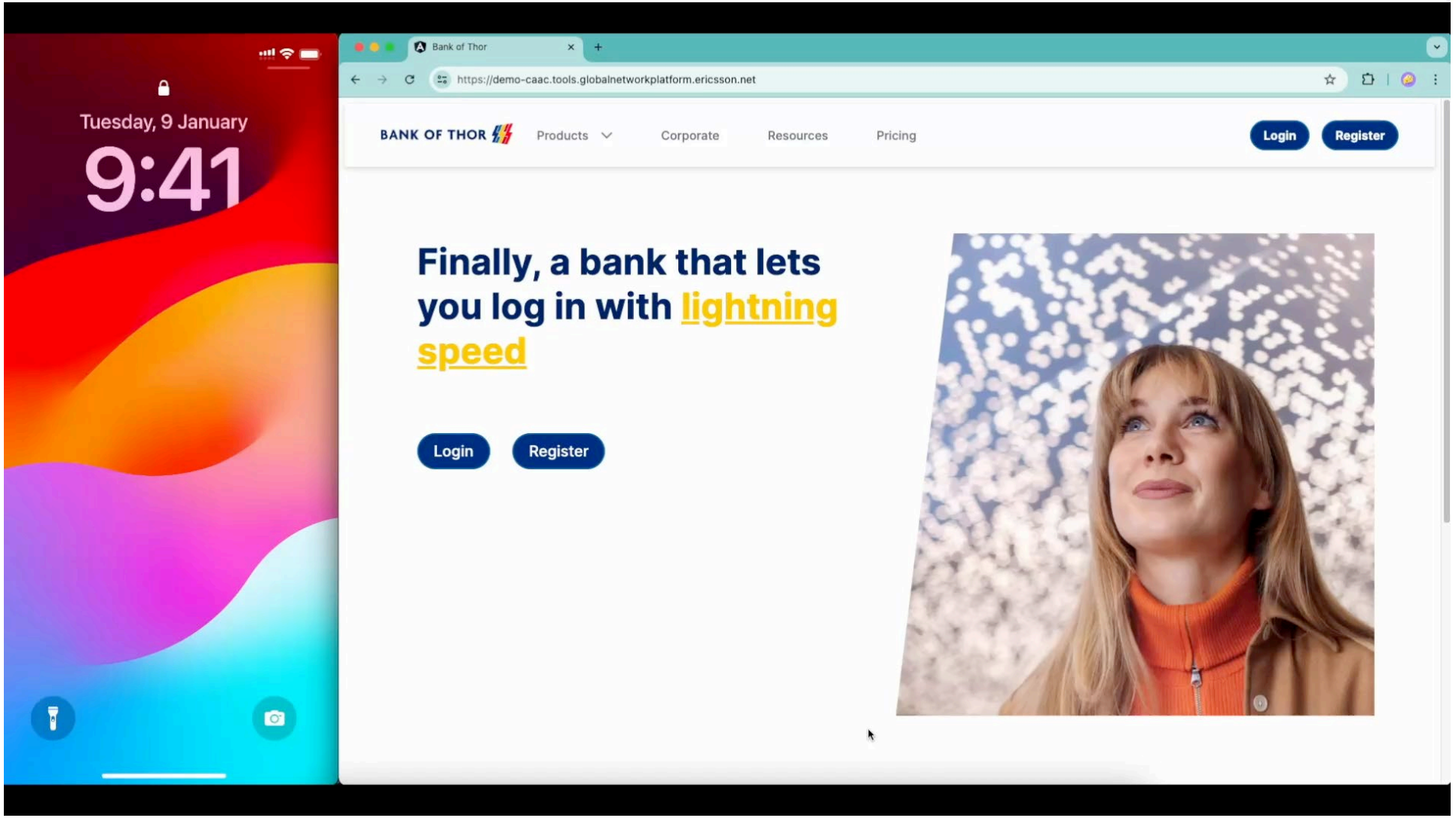
Many Voices.
One Community.

Demo

- Native app scenario
  1. User inserts username/password
  2. App starts verifying phone number
  3. Once it is verified, user is logged-in



Demo - companion device scenario



RSAC™ 2025 Conference

The road ahead

Many Voices.
One Community.

Situation now

CAMARA Number Verification

- Many operators have launched this API to be consumed by applications
  - API deployment world map by GSMA
- Various Communication Platform-as-a-Service(CPaaS) players providing this capability
  - Vonage Number Verification API
- News from the US carriers: AT&T, T-Mobile and Verizon
  - Launching Standard Number Verification API

Enhanced Number Verification (Carrier Token-based)

- Many operators are in process of launching the Enhanced Number Verification
- Google and Firebase are working on API-based phone number verification that is based on carrier tokens (link)
- Work is ongoing also in the CAMARA standardization group for this newer mechanism

Challenges ahead

Getting the ecosystem players to agree on the right things and to deliver on time

- Operators, telecom vendors, device vendors

Economies of scale

- Need sufficiently large market availability to make it attractive

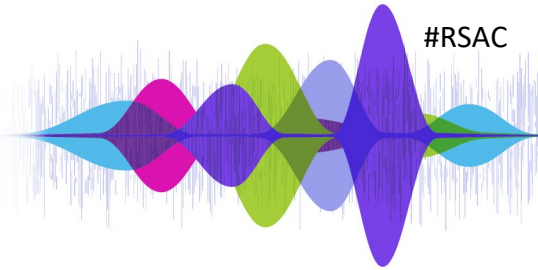
Summary

New number verification APIs will significantly improve the overall security and privacy over SMS OTP

It will bring a significantly better UX into your authentication process

The solution is not to replace the SMS in general but to improve over SMS OTP that is used for 2nd factor authentication

Apply What You Have Learned Today



Next week

- Do a quick analysis of the 2nd factor mechanisms in use within your organization

By 3 months

- Understand how this new method can help your organization with improved security and customer satisfaction

By 6 months

- Start experimenting with the enhanced number verification
- Get your customers' feedback compared to using SMS OTP

RSAC 2025 Conference

Many Voices.
One Community.

Thank You!

Kazi.wali.ullah@ericsson.com

https://www.linkedin.com/in/kaziullah/